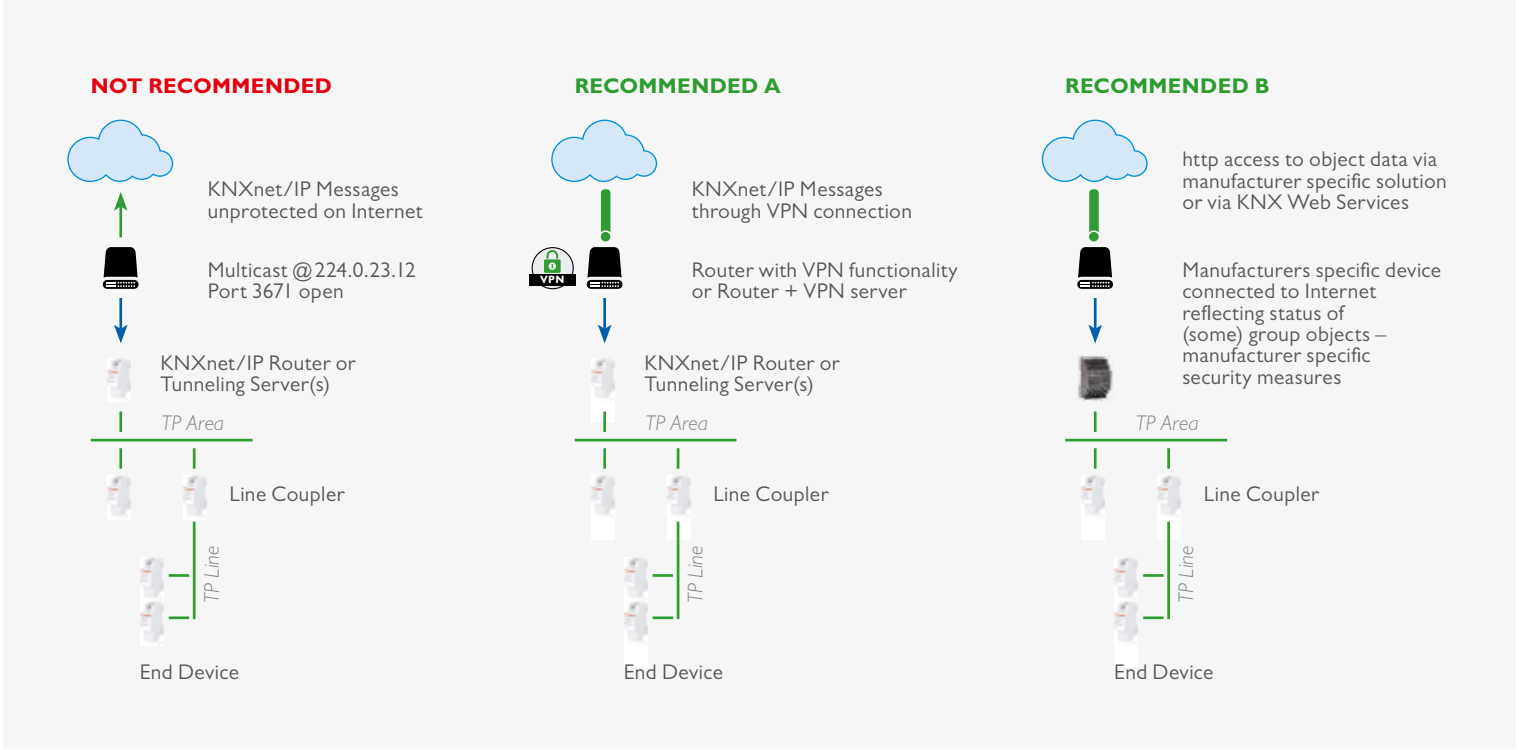
Smart home and building solutions.
Global. Secure. Connected.

KNX SECURE

ARTÍCULO SOBRE LA POSICIÓN DE KNX EN LO QUE RESPECTA A LA SEGURIDAD Y LA PRIVACIDAD DE LOS DATOS

Este artículo tiene como objetivo constituir una guía tanto para los instaladores como para los fabricantes KNX, de manera que conozcan las medidas actuales que se pueden instrumentar para aumentar la seguridad de las instalaciones KNX.

PREVENCIÓN DEL ACCESO A LA RED DE LOS DIVERSOS MEDIOS FÍSICOS KNX



Acceso a las redes KNX a través de Internet

Un adecuado concepto de seguridad se basa en asegurar la debida prevención contra los accesos no autorizados. En el caso de una instalación KNX, esto implica que solo las personas autorizadas (el instalador, el cuidador y el usuario) puedan acceder físicamente a la instalación KNX. Al diseñar e instalar cada medio KNX, los elementos críticos deben protegerse de la mejor materia posible.

Instalación de los cables y los dispositivos

- Por lo general, las aplicaciones y los dispositivos deben fijarse de manera apropiada para evitar que puedan retirarse fácilmente en el caso de que personas no autorizadas accedan a una instalación KNX.
- Los recintos y los cuadros de distribución contentivos de dispositivos KNX deben estar cerrados debidamente o montados en salas a las que solo puedan acceder las personas autorizadas.
- En las áreas al aire libre, los dispositivos deben montarse a una altura suficiente (por ejemplo, estaciones meteorológicas, sensores de viento, detectores de movimientos, etc.).
- En todas aquellas áreas públicas que no cuenten con una vigilancia suficiente, debe considerarse el uso de dispositivos convencionales en relación con las entradas binarias montados en áreas protegidas (cuadros de distribución, por ejemplo) o en interfaces de pulsadores, de manera de evitar el acceso al bus.
- De estar disponibles, deben usarse las medidas antirrobos provistas por ciertos módulos de aplicación (por ejemplo, sujeción de los dispositivos mediante tornillos solo extraíbles mediante herramientas de alta resistencia a la tracción).

Par trenzado

- Los extremos de los cables no deben estar visibles (colgando fuera de la pared (tanto en el interior como en el exterior del edificio).
- El cable de bus en las áreas externas supone un riesgo mayor. En este caso, el acceso físico al cable de par trenzado KNX debe dificultarse aún más que en las viviendas o los edificios.
- Para una protección adicional, los dispositivos instalados en las áreas con una vigilancia limitada (al aire libre, recintos

subterráneos de estacionamiento, salas de baño, etc.) pueden conectarse a una línea adicional. Mediante la activación de la tabla de filtros en los acopladores de línea de conformidad con la cláusula 2, es posible que evitar que los piratas informáticos puedan acceder a toda la instalación.

Línea de potencia

- Deben usarse filtros electrónicos para filtrar las señales entrantes y salientes

Frecuencia

Ya que la radiofrecuencia constituye un medio abierto, no es posible instrumentar medidas de protección física para evitar el acceso. En este caso, las medidas recogidas en las cláusulas 2 a 5 deben instrumentarse (particularmente, las enumeradas en la cláusula 4).

IP

- La automatización de los edificios debe ejecutarse a través de una red de área local (LAN) o una red de área loca inalámbrica (WLAN) dedicada con su propio hardware (enrutadores, conmutadores, etc.).
- Independientemente del tipo de instalación KNX, de todas formas, deben observarse los mecanismos de protección habituales para las redes IP. Estos mecanismos pueden incluir:
  - MAC filters
  - El cifrado de las redes inalámbricas en combinación con contraseñas seguras (cambio de la contraseña por defecto, WPA2 o superior) y la protección de dichas redes de personas no autorizadas.
  - El cambio del nombre de la red (SSID) por defecto por el que el punto de acceso inalámbrico es visible en la red, sobre todo si indica el fabricante y el tipo de producto. Un SSID por defecto puede señalar las debilidades específicas de un producto de los puntos de acceso utilizados y, de esta manera, ser particularmente vulnerables a los piratas informáticos. Además, el punto de acceso puede configurarse de tal manera de evitar la señalización (transmisión del SSID, entre otras cosas).
- En lo que respecta a la multidifusión IP KNX, debe usarse otra dirección IP como determinada (224.0.23.12). Una dirección apropiada puede acordarse con el administrador de la red.
- Es necesaria la participación de los especialistas informáticos en redes en los proyectos de mayor envergadura con conexión a KNXnet/IP: de esta manera, la configuración de la red aún puede optimizarse (conmutadores gestionados, LAN virtual, puntos de acceso con IEEE 802.X, etc.), pudiéndose instrumentar mecanismos de protección adicional como el filtrado de los correos electrónicos y los antivirus.

Internet

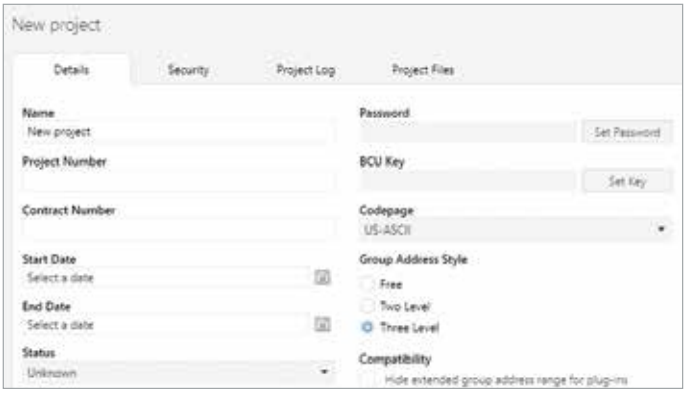
- El enrutamiento KNXnet/IP y la tunelización KNXnet/IP no se han diseñado para su uso a través de internet. En consecuencia, no es recomendable abrir los puertos de los enrutadores a internet, lo que haría visible la comunicación KNX a través de internet.
  - Las instalaciones (W)LAN deben protegerse mediante un contrafuegosIn case no external access to the installation is necessary, the default gateway can be set to 0, in this way blocking any communication to the internet.
  - En el caso de que no se necesite acceso externo a la instalación, la puerta de enlace por defecto puede establecerse en 0, con lo que se bloquea cualquier comunicación a través de internet.
- Cuando alguien desea dar acceso a una instalación a través de internet, lo puede llevar a cabo de la siguiente manera:
  - Asegurando el acceso a la instalación KNX a través de conexiones VPN: no obstante, esto requiere un enrutador compatible con la funcionalidad de servidor VPN o un servidor con funcionalidad VPN.Any of the dedicated manufacturer specific solutions available in the market and visualisations (e. g. allowing http access).
  - Cualquiera de las soluciones específicas del fabricante dedicado disponibles en el mercado y las visualizaciones (por ejemplo, permitiendo acceso HTTP).
  - En una extensión a la Norma KNX, KNX ha especificado una solución KNX normalizada para acceder a las instalaciones KNX a través de internet mediante servicios web.

LIMITACIÓN DE LAS COMUNICACIONES NO DESEADAS EN EL SENO DE LA RED

- Las direcciones individuales de los dispositivos deben asignarse adecuadamente en función de la topología. Además, los enrutadores deben configurarse para no pasar mensajes con direcciones de origen inapropiadas. De esta manera, una comunicación no deseada puede limitarse a una sola línea.
- La comunicación punto a punto y, posiblemente, la comunicación de difusión mediante todos los enrutadores deben bloquearse. De esta manera, una reconfiguración puede limitarse una vez más a una sola línea.
- Los acopladores deben configurarse para usar activamente las tablas de filtros y no pasar las direcciones de grupo que no se usan en una línea específica. De lo contrario, la comunicación insertada en una línea específica entraña el riesgo de extenderse incontroladamente a través de toda la instalación KNX.

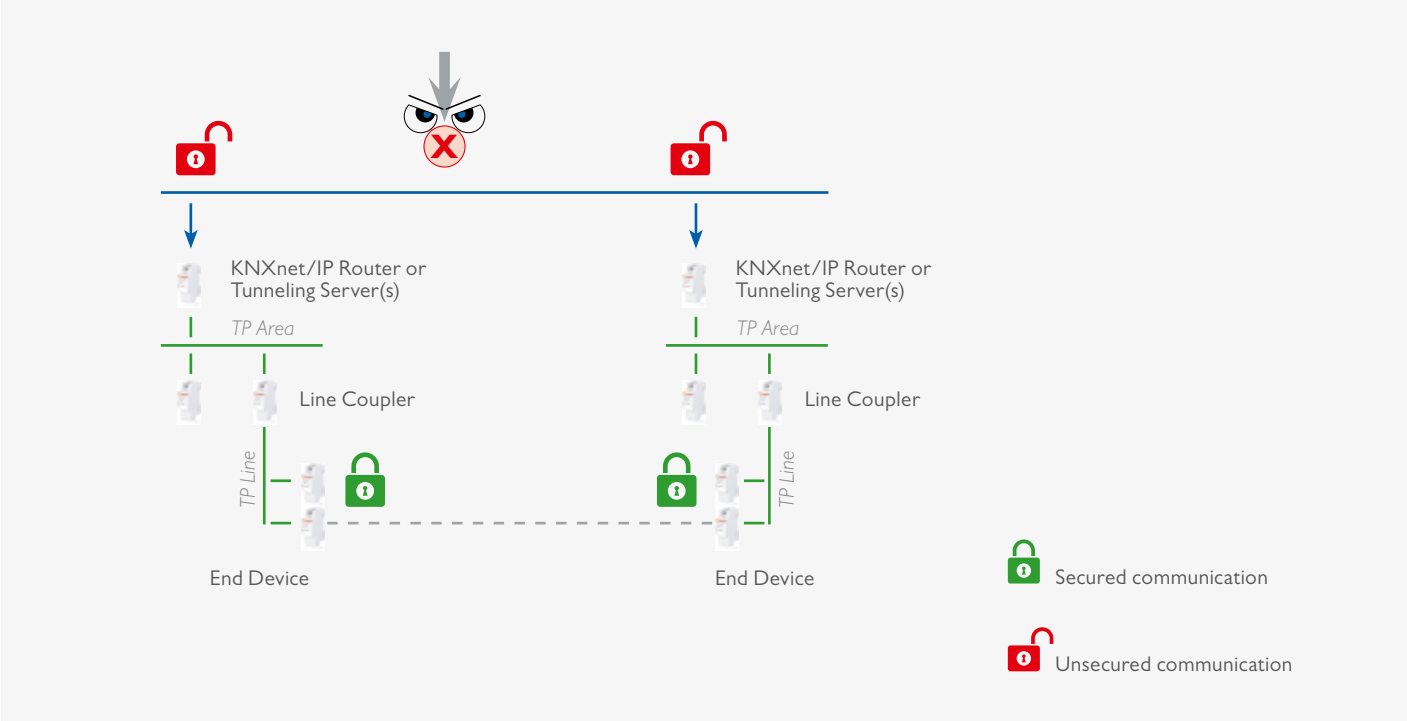
PROTECCIÓN DE LA COMUNICACIÓN DE LA CONFIGURACIÓN

ETS permite definir una contraseña específica para el proyecto mediante la cual se pueden bloquear los dispositivos para evitar accesos no autorizados. Así, se evita que personas no autorizadas puedan leer o modificar la configuración de la instalación.



Protección de la comunicación de la configuración en ETS

PROTECCIÓN DE LA COMUNICACIÓN EN TIEMPO DE EJECUCIÓN



Protecting KNX run time communication on an IP network with KNXnet IP Security

- Además de las medidas antes mencionadas, la comunicación en tiempo de ejecución KNX puede protegerse mediante los mecanismos
  - KNX Data Secure y
  - KNX IP Secure especificados
- KNX Data Secure garantiza que, independientemente del medio KNX seleccionado, los mensajes enviados por los dispositivos KNX se puedan autenticar y/o cifrar. Para garantizarlo, incluso en caso de que tal comunicación no estuviera protegida y tales redes estuvieran conectas al IP, se han definido además los mecanismos KNX IP Secure. De esta manera, se garantiza que la tunelización KNX IP o el enrutamiento de los mensajes no se puedan registrar ni manipular en IP. Los mecanismos KNX IP Secure garantizan que una envoltura de seguridad se añada alrededor de todo el tráfico de datos KNXnet/IP.
- Los mecanismos KNX Data Secure y KNX IP Secure garantizan que los dispositivos puedan establecer, de este modo, un canal de comunicación protegida que garantice:
- La integridad de los datos, es decir, evitar que un pirata

informático se haga con el control inyectando tramas. En KNX, esto se garantiza añadiendo un código de autenticación a cada mensaje: este código añadido permite verificar que el mensaje no ha sido modificado y que se origina efectivamente del socio de comunicación de confianza.

- Actualización, es decir, evitando que un atacante registre tramas y las reproduzca posteriormente sin manipular el contenido. En KNX Data Secure, esto se garantiza mediante un número de secuencia y en KNX IP Secure mediante un identificador de secuencia.
- Confidencialidad, es decir, cifrando el tráfico de la red para garantizar que un atacante tenga el menor conocimiento posible de los datos que se transmiten en cualquier momento. Al permitir el cifrado de la red KNX, los dispositivos KNX garantizan al menos un cifrado de conformidad con los algoritmos AES-128 CCM junto con una clave simétrica.

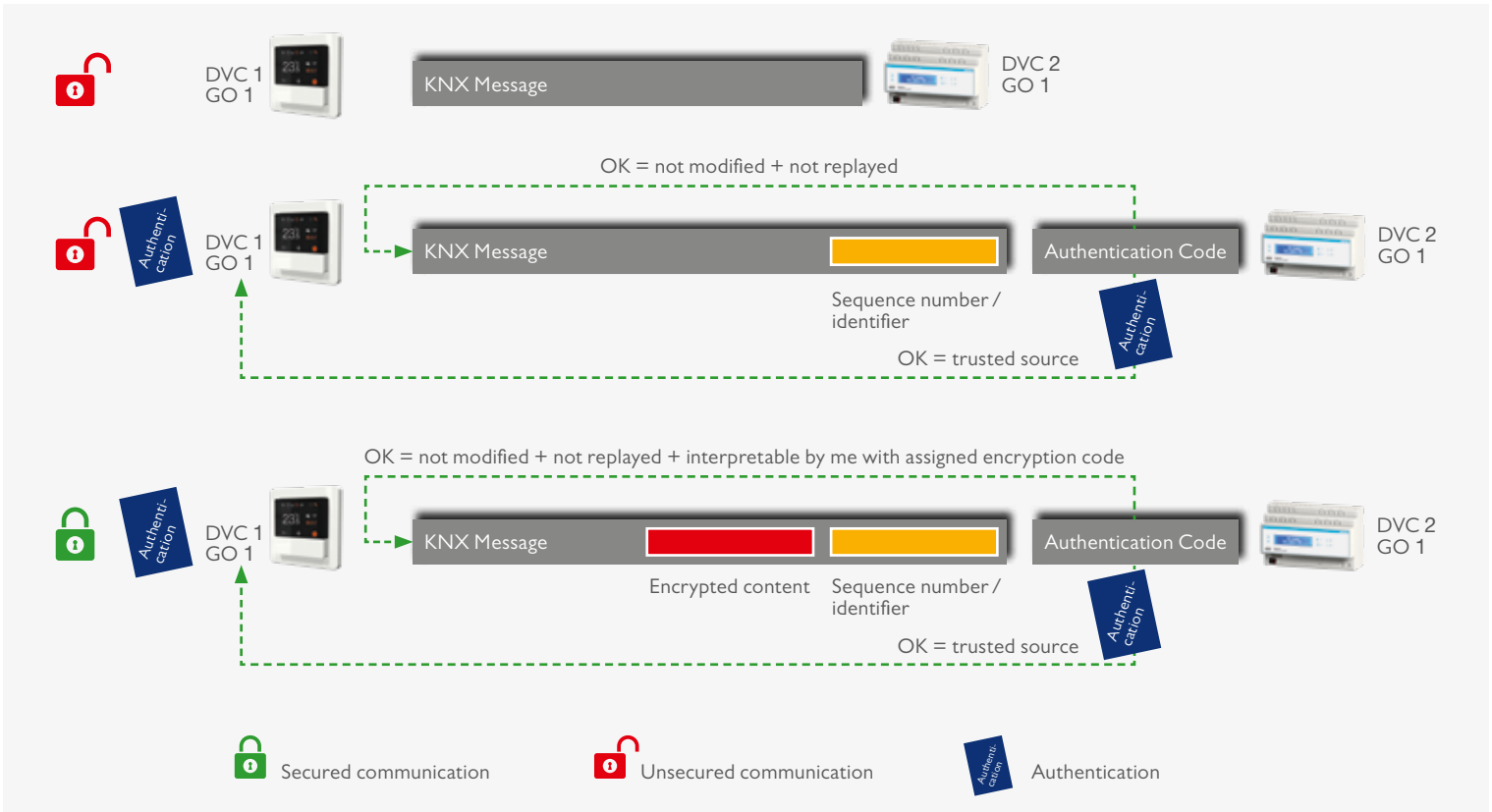
Una clave simétrica supone que tanto el remitente como los destinatarios utilizan la misma clave. En el caso del remitente, para proteger el mensaje saliente (autenticación y confidencialidad) y en el caso de los destinatarios, para verificar cuando se recibe dicho mensaje.

Los dispositivos KNX Data Secure usan un formato de telegrama KNX más largo al transmitir los datos autenticados y cifrados. Esto no afecta en absoluto la velocidad de reacción de los dispositivos. En cuanto a KNX Data Secure, los dispositivos están protegidos de la siguiente manera:

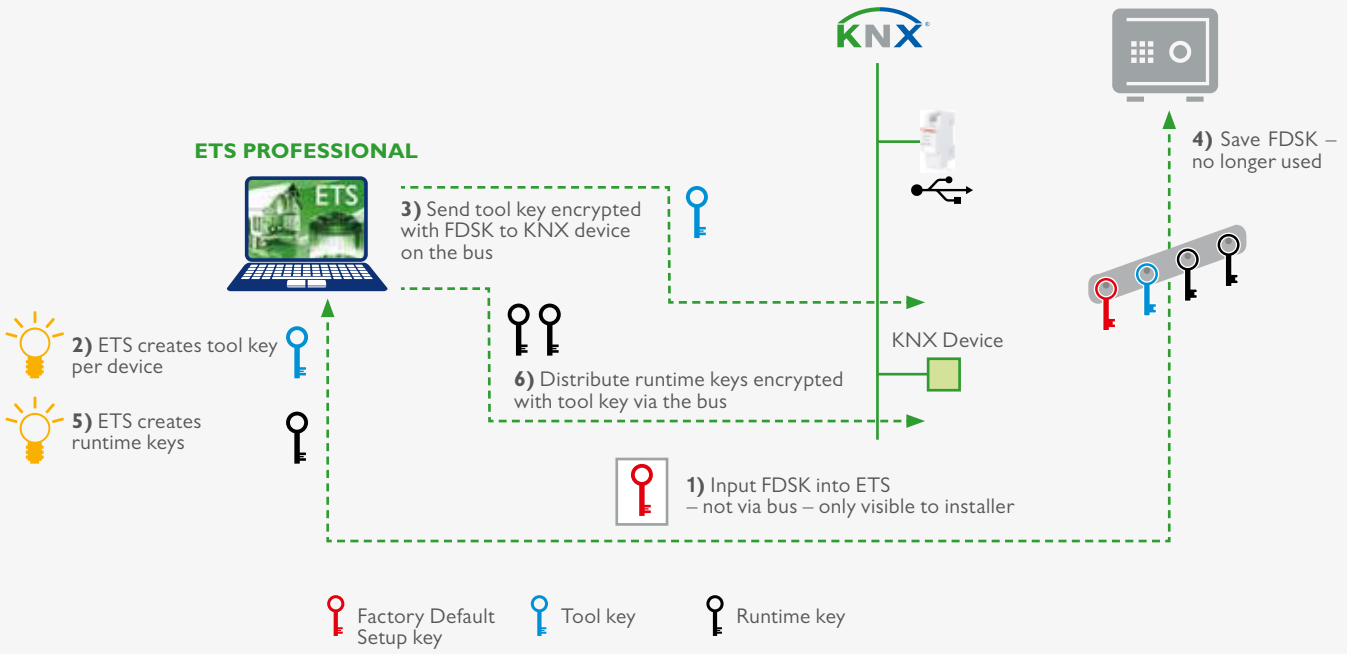
- Los dispositivos se envían con una única clave de configuración de dispositivo de fábrica (FDSK).
- El instalador introduce esta FDSK en la herramienta de configuración de ETS (en cualquier caso, esta acción no se realiza mediante el bus).
- La herramienta de configuración crea una clave de herramienta específica del dispositivo.
- Mediante el bus, el ETS envía su clave de herramienta al dispositivo que se va a configurar; no obstante, cifra y autentica este mensaje con la FDSK introducida anteriormente. Ni la herramienta ni la FDSK se transmiten en ningún momento como texto sin formato en el bus.
- A partir de ese momento, el dispositivo solo acepta la clave de herramienta para una configuración adicional con el ETS. La FDSK se deja de usar durante las comunicaciones posteriores, a menos que se restablezca la configuración de fábrica del dispositivo, tras lo cual, se borrarán todos los datos protegidos que contenga.
- El ETS crea claves en tiempo de ejecución (tantas como sean necesarias) para las comunicaciones de grupo que requieren protección.
- Mediante el bus, el ETS envía estas claves en tiempo de ejecución al dispositivo que se va a configurar; no obstante, cifra y autentica estos mensajes con la clave de herramienta. Las claves en tiempo de ejecución nunca se transmiten como texto sin formato en el bus.

En cuanto a KNX IP Secure, se establece una conexión segura (tunelización o gestión de dispositivos) de la forma siguiente:

- Tanto el cliente como el servidor crean un par de claves públicas/privadas individuales. Esto es lo que se conoce como cifrado asimétrico.
- El cliente envía su clave pública al servidor como texto sin formato.
- El servidor responde con su clave pública en texto sin formato, con el resultado del cálculo siguiente añadido: calcula el valor XOR de su clave pública del servidor con la clave



Resumen de los mecanismos de KNX Data Secure



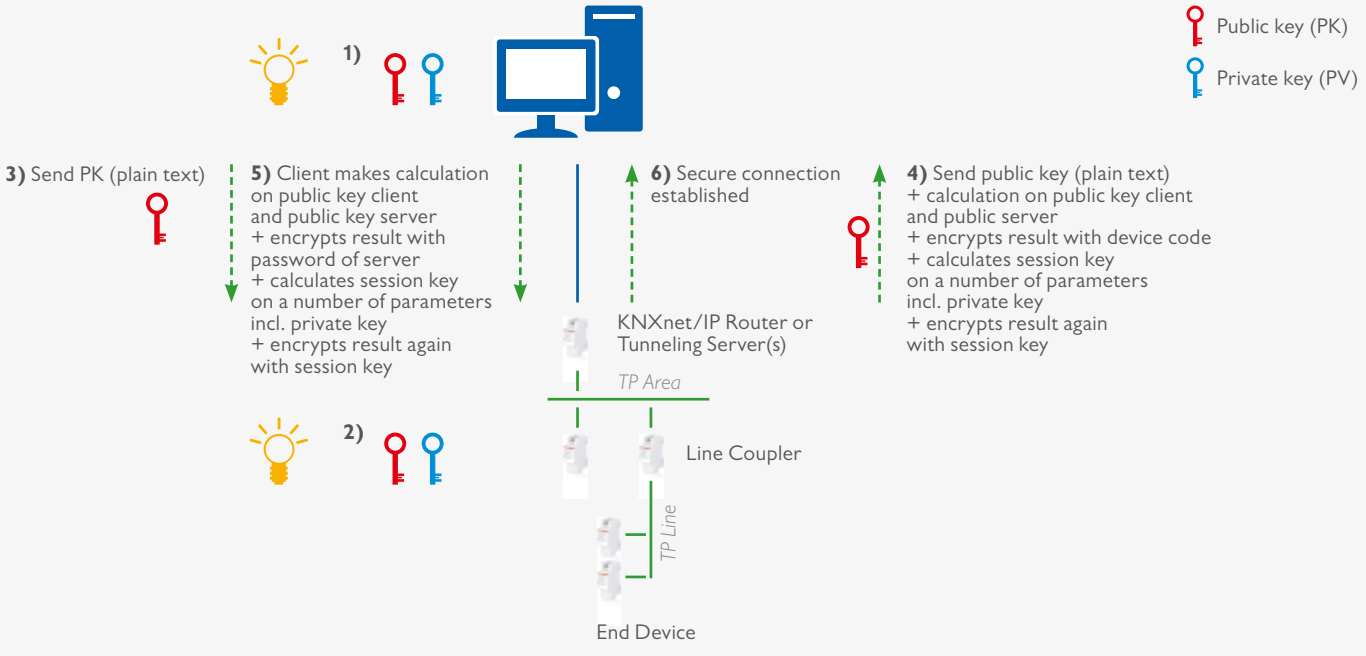
Procedimiento para proteger los dispositivos KNX

pública del cliente, cifra esto con el código del dispositivo para autenticarse con el cliente y cifra esto por segunda vez con la clave de sesión calculada.

- Ora el ETS durante la configuración, ora la clave de herramienta asigna el código de autenticación del dispositivo. El operador de la visualización que desea establecer una conexión segura con el servidor pertinente debe proveer dicho código de autenticación del dispositivo.
- El cliente realiza la misma operación XOR; no obstante, se autoriza a sí mismo cifrando primeramente esto con una de las contraseñas del servidor y otra vez, por segunda vez, con la clave de sesión. Cabe destacar que el algoritmo de cifrado utilizado (Diffie-Hellmann) garantiza que las claves de sesión del cliente y la del servidor sean idénticas. El operador de la visualización que desea establecer una conexión segura con el servidor pertinente debe proveer las contraseñas del servidor.

En cuanto a las medidas descritas anteriormente para proteger la comunicación en tiempo de ejecución, cabe señalar que:

- Los dispositivos KNX Data Secure pueden usarse sin ningún problema junto a los dispositivos KNX «clásicos». Esto implica que KNX Data e IP Secure pueden instrumentarse como medidas de seguridad adicional.
- Si el instalador opta por usar un dispositivo KNX IP Secure en una red troncal IP, todos los acopladores IP y cualquier dispositivo KNX IP en esta red troncal deben ser del tipo KNX IP Secure.
- Si un instalador ha usado —por solicitud de un cliente— un dispositivo KNX Secure con respecto a una función para asegurar la comunicación en tiempo de ejecución, cada socio de



Setting up a KNX IP Secure Connection

comunicación de este dispositivo también debe ser compatible con KNX Secure con respecto a la función vinculada. En otras palabras, un objeto de comunicación de un dispositivo KNX Secure no puede vincularse una vez a una dirección de grupo protegida y una vez a una dirección de grupo sin formato.

Los dispositivos que admiten KNX Data e IP Secure se pueden distinguir de los dispositivos KNX «clásicos» gracias a la indicación «X» en su etiqueta.
KNX IP Secure y KNX Data Secure son compatibles a partir de ETS 5.5. El ETS permite configurar nuevos dispositivos KNX Secure y reemplazar dispositivos KNX Secure defectuosos.

ACOPLAMIENTO DE KNX A LOS SISTEMAS DE SEGURIDAD

El acoplamiento de KNX a aplicaciones tales como sistemas antirrobos, de detección de incendios y apertura de puertas se puede garantizar mediante:

- Interfaces o dispositivos KNX debidamente certificados por las empresas aseguradoras locales de pérdidas.
- Contactos libres potenciales (entradas binarias, interfaces de pulsadores, etc.).
- Interfaces apropiadas (RS232, por ejemplo) o puertas de enlace: en este caso debe garantizarse que la comunicación KNX no pueda activar las funciones pertinentes de seguridad en la parte correspondiente a la seguridad de la instalación.

DETECCIÓN DE ACCESOS NO AUTORIZADOS AL BUS

Obviamente, el bus podría monitorizarse y el tráfico no habitual podría rastrearse.
Los dispositivos KNX Secure mantienen un control de los piratas informáticos en los registros de errores de seguridad: de esta manera, en cualquier momento, es posible comprobar si la instalación KNX ha sido objeto de ataques de seguridad.
Algunos tipos de dispositivos pueden detectar si otro dispositivo envía telegramas con su dirección individual. Esto no se anuncia espontáneamente en la red; no obstante, puede leerse en el PID_DEVICE_CONTROL.
Una instrumentación muy reciente ya puede exhibir el PID_DOWNLOAD_COUNTER.
Al comparar la lectura (periódicamente) con un valor de referencia, se señalarán los cambios en la configuración del dispositivo.

CUMPLIMIENTO DEL RGPD DE LA UE

RGPD es la abreviatura de Reglamento General de Protección de Datos (consulte la página web https://ec.europa.eu/info/law/law-topic/data-protection_es).
El reglamento tiene como objetivo armonizar las leyes en materia de protección de datos de toda Europa.
Con miras a cumplir con el Reglamento General de Protección de Datos (RGPD), el instalador debe entregar al cliente el archivo del proyecto ETS. Tanto el instalador como el cliente deben firmar una declaración de protección de datos.
Los datos generados por los dispositivos KNX solo pueden usarse con el propósito de controlar a distancia el dispositivo por parte del cliente (mediante la aplicación), con fines de diagnóstico y para el desarrollo adicional de productos. No pueden usarse con miras a hacer publicidad personalizada.

Bibliografía

[1] AN 158 KNX Data Security
[2] AN 159 KNX IP Secure
[3] Volume 3/8/x KNXnet/IP Specifications

Smart home and building solutions.
Global. Secure. Connected.